REMARKS

The present remarks are in response to the Final Office Action dated June 22, 2009, in which the Office Action issued a rejection of claims 21-25, 27-29, 31-32, 38 and 40-45. In this response, Applicant responds to the present Final Office Action with amended claims, remarks, the requested Substitute Specification, and respectfully requests that the pending claims be placed in a state of allowance. No new matter has been added.

A. Amended Claims

Claims 21, 25, 27-29, 31, 35, 38, and 40 have been amended. Claims 46-48 have been added. Support for claims 46-48 can be found in paragraphs 30, 70 and 79 (i.e., with reference to the countdown timer) for "pseudo-real time" and throughout the specification (see, e.g., paragraphs 107 and 110-113) for downstream transmission to one or more network devices.

B. Withdrawal of Finality of Rejection

In the Final Office Action, the Examiner rejected claims 21-25, 27-29, 31-32, 38 and 40-45. If an Applicant files a Request for Continued Examination (RCE) in a timely manner as set forth in 37 CFR 1.17(e) with a submission, the Office will withdraw the finality of any Office Action to which a reply is outstanding and the submission will be entered and considered. See 37 CFR 1.114(d).

Although the Applicant disagrees with the Examiner's grounds of rejection, the Applicant has added dependent claims 46-48. These claims recite pseudo-real time and downstream transmission. As the Examiner indicated in the most recent Advisory Action, dated September 28, 2009, these limitations will require further search and consideration.

Accordingly, the Applicant respectfully requests that the Examiner withdraw the finality of the recent Office Action, dated June 22, 2009. Further, in view of the Amendments and Remarks submitted herewith, the Applicant respectfully requests that the pending claims be placed in a state of allowance. No new matter has been added.

C. Priority

The Examiner stated that Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 USC §119(e). The Examiner further stated that Applicant must file a petition under 37 CFR §1.78(a) for an unintentionally delayed benefit claim of benefit under 35 USC §120. The requested petition was filed on February 19, 2009, and a decision by the Office of Petitions granting the Applicant's priority request was mailed on September 23, 2009.

The Office of Petitions stipulated that "all other requirements under 35 U.S.C. §§120 and 1.78(a)(1) and (a)(2) and under 35 U.S.C. §119(e) and 37 CFR 1.78(a)(4) and (a)(5) must be met." With regard to the requirements remaining under 35 U.S.C. §120 and 37 CFR §§1.78(a)(1) and (a)(2), the prior-filed nonprovisional Application No. 09/899,559 names as an inventor at least one inventor named in the instant (later-filed) Application No. 10/681,034—i.e., Michael A. Kerr. The instant application further discloses the named inventor's invention in its claims. Finally, the prior-filed Application No. 09/899,559 is entitled to a filing date as set forth in 37 CFR §1.53(b), and the filing fee set forth in §1.16 was paid within the pendency of the application.

With regard to the requirements remaining under 35 U.S.C. §119(e) and 37 CFR§§ 1.78(a)(4) and (a)(5), the prior-filed provisional Application No. 60/266,956 names as an inventor at least one inventor named in the later-filed Application No. 09/899,559—i.e., Michael A. Kerr. The later-filed Application further discloses the named inventor's invention in its claims. The prior-filed provisional Application No. 60/266,956 is further entitled to a filing date as set forth in 37 CFR §1.53(c), and the filing fee set forth in §1.16(d) was paid within the time period set forth in §1.53(g). Finally, the later-filed Application No, 09/899,559 was amended on April 23, 2002 to contain the required reference to the prior-filed Application No. 60/266,956 in the Specification.

Accordingly, having now demonstrated compliance with all legal and regulatory requirements, the Applicant respectfully requests that the Examiner enter the benefit claim under 35 U.S.C. §120 to prior-filed nonprovisional Application No. 09/899,559 and under 35 U.S.C. §119(e) to the prior-filed provisional Application No. 60/266,956.

D. Specification

Copies of the Substitute Specification (with and without markings) have been included as attachments as required by the Examiner. ***The Substitute Specifications contain no new matter***.

As approved by the Office of Petitions, the first sentences of the specification under the title have been edited to include cross references to provisional application number 60/266,956 and to non-provisional application 09/899,559.

E. Anticipation Rejections (35 U.S.C. § 102)

The Examiner has rejected claims 21-25, 28-29, 35-36, 38 and 41-45 under 35 USC 102 (b) as being anticipated by Applicant's published patent Application No. 2002/0142844. As explained above, the Applicant properly claimed priority under 35 U.S.C. §120 to prior-filed nonprovisional Application No. 09/899,559 and under 35 U.S.C. §119(e) to the prior-filed provisional Application No. 60/266,956.

Applicant therefore respectfully requests that the Examiner withdraw the portion of the rejection based on Application No. 2002/0142844.

F. Obviousness Rejections (35 U.S.C. § 103)

The Examiner has rejected claims 21-25, 28-29, 35-36, 38 and 41-45 under 35 U.S.C §103(a) as being unpatentable over Tulley *et al.* (U.S. 6,719,631, hereinafter, "Tulley") in view of Walker *et al.* (U.S. 6,001,016, hereinafter, "Walker"). For the reasons set forth below, the Applicant disagrees with the Examiner's grounds of rejection.

1. Tulley *et al.* do not teach a gaming server configured to generate a random game output

The Examiner asserts that Tulley disclose a gaming system and method comprising a gaming server that can generate a "random output" (4:37-54, 6:20-23, 26-61, 7:26-34, 8:18-22, 8:30-9:7). The Applicant respectfully disagrees.

Tulley teach the use of event parameters for a gaming system with predetermined and pre-stored event results (6:38-53). Further, Tulley teach the use of event parameters (e.g., total wager amount, total number of events, event wager amount) to enhance remote lottery systems. These lottery systems enable players to purchase "scratch-off" style lottery game outcomes from a central computer (2:8-16). Additionally, Tulley teach randomly allocating a total payout amount over the number of games that a player has chosen to play. 16:7-10.

However, Tulley do not teach a gaming server configured to generate a random game output. Rather, the systems and methods described by Tulley are directed to class 2 (lottery) systems, wherein predetermined and pre-stored event results are transmitted to a client device. Consider the example provided at column 6, lines 26-53. Tulley teach an event result server configured to transmit a set of predetermined results to a controller. Further, the set of predetermined event results, Tulley explain, may be received by the controller on an incremental basis—e.g., once each week. Thus, this example clarifies that Tulley is directed to a class 2 lottery style system, where an RNG is not used to generate a random game output.

On balance, Tulley also state, "the controller 300 may initiate a random number generation process and determine that the player will win twenty-five dollars based on a thirty dollar total wager amount." (6:20-23. Emphasis added). At column 17, lines 7-8, Tulley also state, "According to another embodiment, the controller 300 uses a random outcome to determine the total payout amount." (Emphasis added). These statements would not have suggested (and certainly they fail to teach) using a server to generate random game outputs for two reasons: (1) Tulley is generally directed to class 2 gaming, and it would not have been clear based on the examples provided and the bulk of the disclosure what alteration to the disclosed class 2 system these blanket statements were intended to set forth, particularly in view of the fact that an alteration requiring the use of a random number generator would alter the operation of the basic system such that reclassification as a class 3 device would be required; and (2) the statements provided by Tulley are not clearly directed to randomly determining individual game outcomes; indeed, both statements suggest that a random outcome may be used to determine the "total payout amount." Thus, the Applicant respectfully submits that Tulley simply fail to disclose a primary element of the independent claims—generating random *game outputs* on a server.

Finally, the Examiner argues at page 11, line 13, that it would have been obvious to combine the Tulley system with the system disclosed in the Walker reference "for the predictable result of ***determining a particular game outcome output***." However, Tulley disclose a batch process (i.e., generating a set of predetermined and pre-stored event results) for determining game outcomes. Therefore, the Examiner's finding that it would have been obvious to combine Walker with Tulley "to achieve the result of determining a particular game outcome" (emphasis added) suggests that the Examiner also believes that Tulley discloses a class 2 system that determines game outcomes in pre-stored batches. Otherwise, the combination of Walker for the advantage of determining a "particular…outcome" would be unnecessary.

2. Tulley *et al.* do not teach a paytable module

The Examiner states, "Tulley discloses a gaming system and method with gaming server that comprises a paytable module…" (See final rejection, page 10, lines 16-17). The portions of the reference cited by the Examiner, however, are directed to total payout amounts. The Applicant respectfully submits that a total payout amount is markedly different from a paytable. Indeed, a paytable is a table showing for each bet combination how much money a player will win on a particular game given a certain game outcome. A total payout amount, as specified in Tulley, describes the payout over a number of games. Thus, the Applicant respectfully submits that Tulley do not teach a paytable module (nor even a paytable), let alone such a module residing on a server.

3. It would not have been obvious at the time of invention to combine Tulley *et al.* with Walker et al., because the Examiner's rationale for combining the references is inadequate

The Examiner relies on Walker for a server that "generates a visual representation of a payout outcome for transmission to [a] gaming device" (see final rejection, page 11, lines 5-7). However, the Examiner's rationale for combining Walker with Tulley is inadequate to support the rejection. First, the Examiner states that the combination would have been obvious "to improve the gaming system and method of Tulley for the expected result of maintaining central control of game outcome ***to increase security***." (Emphasis added. See final rejection, page 10, lines 2-15). The Applicant respectfully submits that nowhere is Walker directed to, nor does the reference even mention, maintaining central control as a means of increasing security. Indeed, the problem addressed by Walker is as follows: "there exists a need for a method and system for remote wagering and play of a gaming device, particularly a method and system that does not require human intervention and live video transmission of the game being played." (Emphasis added. 2:46-50). Thus, Walker do not speak to security. The Applicant respectfully submits, therefore, that it would not have been obvious to combine Walker with Tulley for the purpose of increasing security, as nowhere does Walker state such an advantage resides in their disclosed system.

Moreover, Walker actually teach away from the claimed invention, because the claimed invention is directed to live video transmission of the game being played and Walker specifically state that an advantage of their system is that it does not require "live video transmission of the game being played." A person of ordinary skill, reading Walker, would not have been motivated, nor felt any suggestion, to combine the system taught by Walker with the system taught by Tulley. Again, the combination would not have been obvious.

The Examiner additionally argues that the combination would have been obvious "for the predictable result of ***determining a particular game outcome output***." (See page 11, line 13). Here, the Examiner's rationale is based on hindsight. Once more, there is no teaching, suggestion, or motivation in Tulley or Walker for modifying the Tulley system such that it was capable of generating particular (random) game outcomes. The rationale explicated by the Examiner merely constitutes an advantage, or feature, of the claimed invention—i.e., generating random game outputs (for downstream transmission in real time or pseudo-real time). Under *KSR*, the Court has warned against reliance upon hindsight reasoning. See *KSR International Co. v. Teleflex Inc. (KSR)*, 82 USPQ2d 1385, 1397 (2007), explaining that, "A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning. See *Graham*, 383 U.S. at 36 (warning against a 'temptation to read into the prior art the teachings of the invention in issue'...)" In view of these arguments, the Applicant respectfully submits that the Examiner's rationale for making the Tulley-Walker combination is based on hindsight reasoning, a rationale admonished even under *KSR*.

4. The combination of Walker *et al.* with Tulley *et al.* would change the principle of operation of Tulley *et al.*

The Examiner's suggested combination would change the principle of operation of the Tulley system. As the MPEP clarifies, "[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious." *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

Here, the Applicant respectfully submits that the principle of operation embodied in the Tulley system is that of a class 2 gaming system, whereby a plurality of pre-stored and pre-determined outcomes are transmitted in sets or batches to a wireless gaming device. As the Examiner points out (see above), the combination of Walker is necessary to accomplish a modified version of the Tulley system capable of determining particular game outcome outputs. However, any such modification of the Tulley system would transform the principle of operation underlying the system--i.e., it would attempt to make the Tulley system send real time game outcomes to a handset, as opposed to batches of predetermined game outcomes. This is a fundamental alteration to Tulley, because the Tulley system does not transmit game outcomes in real time; rather, it operates like a "lottery," sending large sets of results to periodically connected (as opposed to currently connected) devices.

5. Walker *et al.* do not teach—implicitly or explicitly—an encoder

The Examiner contends that Walker "implicitly" disclose an encoder. (See Examiner's final rejection, page 9, lines 14-16). More particularly, after citing numerous and broad swaths of text in Walker, the Examiner states that the claimed encoder is "implicit for wireless transmission/reception" *Id*. Moreover, the Examiner's only physical reference to the claimed encoder is element 284, which corresponds to a payout table in Walker; the Applicant respectfully submits that a payout table has nothing to do with an encoder—and, certainly, a table does not imply an encoder. With regard to the Examiner's statement that an encoder is implicit for wireless communication, the Applicant observes that that Examiner has failed to show where Walker implies an encoder. Further, the Applicant respectfully submits that it is inappropriate to suggest that a claim limitation is implicit in a broad area of technology, e.g., wireless communications. Of course, it may be that a claim limitation is implicit in a reference; however, once more, the Walker reference does not imply the use of an encoder. Indeed, Walker is silent as to the details of the wireless communication mechanism. The reference does not mention MPEG or any other encoding mechanism.

The Examiner has also rejected claims 27, 31, 32, 34 and 40 under 35 U.S.C. 103(a) over Tulley in view of Walker and further in view of Bradford or Schneier (U.S. 5,768,382). For the reasons set forth below, the Applicant disagrees with the Examiner's grounds of rejection.

6. In light of the recently established priority date, Bradford is unavailable as a reference, and it would not have been obvious at the time of invention to combine Tulley, Walker and Schneier to make the claimed invention

First, with regard to the citation to Bradford, the Applicant observes that the citation does not include a patent or publication number identifying the reference;

additionally, the Examiner has not cited a reference to Bradford in the recent form PTO-892. Reviewing the file history, the Applicant notes that the Examiner has, in previous forms PTO-892, cited U.S. Patent 6,709,333 to Bradford, which has a filing date of April 14, 2003 as well as U.S. Patent 6,612,928, filed July 17, 2001. Both patents claim priority to U.S. provisional Application No. 60/300,029, filed June 20, 2001.

However, irrespective of the reference the Examiner intended to cite, the Applicant observes that both Bradford references ('333 and '928) are no longer available under 35 U.S.C. §102 in view of the recent decision by the Office of Petitions regarding the priority date of the instant application. The Applicant therefore respectfully requests that the Examiner withdraw any rejection based upon Bradford.

Turning now to Schneier, the Examiner recently rejected claims 27, 31, 32, 34 and 40, stating that for these cited claims, Tulley in view of Walker discloses all features/steps of the claims reciting a gaming system and method except a smart card, a MAC and cryptographic keys which are used to encrypt/decrypt communications between the verification system and each of the network access devices. The Examiner further stated that Schneier (12:20-25, 15:11-58, 16:13-54, 17:43-63, 23:9-37, 23:53-24:51, 27:28-28:27 disclose a gaming system or method including a remote wireless network access device such as a PDA using two factor authentication input. Therefore, according to the Examiner, it would have been obvious to add a smart card, a MAC or cryptographic keys as taught by Schneier to a gaming system and method of Tulley in view of Walker to increase security or to ensure a user is authorized.

First, as a threshold matter, the Applicant observes that it would not have been obvious to one of ordinary skill at the time of invention to combine Schneier with the proposed Tulley-Walker combination, because, as explained above, the proposed Tulley-Walker combination would not have been obvious. In other words, it would not have been obvious to add an additional reference to the already nonobvious combination proposed by the Examiner.

Second, it would not have been obvious, as the Examiner alleges, to incorporate the teachings of Schneier in the proposed Tulley-Walker combination, because Schneier is directed to a system and method for "remote[ly] auditing" game results in a tournament gaming environment as a means of certifying a plurality of game scores (1:9-12). That is, Schneier is a reference in a field different from that of the Applicant's endeavor. Moreover, the teachings of Schneier would not have been reasonably pertinent to a person of ordinary skill in the art at the time of invention, because it would not logically have commended itself to an inventor with knowledge of Tulley and Walker. See MPEP 2141.01(a). This is so, because both Tulley and Walker already disclose security mechanisms. For instance, Tulley state a need to "register" a remote device with a Web-based system (4:37-38), and Walker disclose a method of verifying both a gaming machine as well as a user—i.e., by way of a unique machine ID and a player tracking card (4:39-59). Thus, Schneier is not analogous art. Beyond that, however, even if Schneier may be construed as analogous art, it still would not have been obvious to a person of ordinary skill to seek out a third reference for additional information regarding authentication, as both Tulley and Walker already disclose methods for performing authentication.

G. Brief Summary of Arguments

Tulley do not teach a gaming server configured to generate a random game output. Rather, Tulley teach a gaming server configured to generate pre-stored and predetermined event results. Tulley disclose randomly allocating a total payout amount. However, a randomly allocated total payout amount is *not* equivalent to a random game outcome.

The Examiner's rationale for modifying Tulley in view of the Walker reference supports the validity of this observation. To be sure, the Examiner reasoned in the recent rejection that it would have been obvious at the time of invention to combine Walker with Tulley in order "to determine a particular game outcome output." As set forth above, however, the recent rejection is inconsistent, in that it first asserts that Tulley teach a gaming server configured to generate random game outputs, and second, that it would have been obvious to combine Walker to make a system capable of generating particular (random) game outputs. In other words, if it would have been obvious to combine a Walker to achieve random game outputs, then Tulley must not teach this aspect of the claimed invention.

Tulley do not teach a paytable module. Rather, the portions of the reference cited by the Examiner are directed to total payout amounts. A total payout amount is a percentage return on an amount wagered.

It would not have been obvious to combine Walker with Tulley to make the claimed invention, first, because Walker do not teach that their system increases security. Second, Walker teach away from the claimed invention, because they indicate that their system does not require live transmission of video data—a primary advantage of the instant invention. Third, it would not have been obvious to make the proposed combination, because the rationale supplied by the Examiner (i.e., that it would have permitted the Tulley system to determine particular game outcome outputs) is based on hindsight; that is, the rationale supplied by the Examiner is a restatement of an advantage of the instant invention.

Thus, neither reference, alone or in combination, teaches the claimed system. Further, there is no suggestion in either reference that a combination would have been, or might have been, advantageous. Further still, a person of ordinary skill, reading the Tulley reference, would neither have been motivated to seek a method for increasing security, nor a method for determining particular game outcome outputs. Indeed, even if a person of ordinary skill had been motivated to increase security in Tulley, Walker would not have constituted an apposite reference, as it makes no mention of security. Finally, there is no rational underpinning supplied for the assertion that a person of ordinary skill would have incorporated Walker in Tulley in order to determine a particular game outcome output beyond a mere restatement of an advantage of the claimed invention. Even under *KSR*, more is required.

The combination of Walker with Tulley would further alter the fundamental principle of operation of the Tulley system—namely, it would transform Tulley from a class 2 lottery system, configured to generate predetermined and pre-stored event results, into a class 3 gaming system, configured to generate real-time or pseudo-real time results based upon a player's input selections.

Walker do not teach an encoder. The Examiner asserts that an encoder is implicit in Walker. However, the Examiner has failed to indicate where, in the

Walker disclosure, an encoder is implied. A payout table (284) does not imply an encoder.

With regard to the rejections made pursuant to the Bradford and Schneier references, Bradford is no longer available under Section 102 (pursuant to the decision by the Office of Petitions), and it would not have been obvious to combine Schneier with Tulley-Walker, because (1) Tulley-Walker was not obvious, and (2) both Tulley and Walker disclose authentication methods; thus, a person of ordinary skill would not have been motivated (and there is no suggestion or other rationale supplied by the Examiner) to seek out additional authentication systems and methods.

F. Conclusion

For all the foregoing reasons, allowance of the pending claims is respectfully requested.

Respectfully Submitted;

Dated: February 26, 2010

James W. Henson
Reg. No. 65,118

James W. Henson
KERR IP GROUP, LLC
9490 Gateway Dr. #104
Reno, Nevada 89521
Ph. 775-841-3388
Fx. 775-841-3389
james@kipg.com

SUBSTITUTE SPECIFICATION (with Markings)

This Substitute Specification with markings contains no new matter.

WIRELESS ~~BIOMETRIC~~ BROADBAND GAMING SYSTEM AND METHOD

CROSS REFERENCES TO RELATED APPLICATIONS

[0001] This patent application is a continuation of patent application 09/899,559 having a filing date of July 5, 2001, now abandoned, which claims the benefit of provisional patent application 60/266,956 filed February 6, 2001. ~~in part of provisional patent application 60/266,856 filed on Feb. 6, 2001.~~

BACKGROUND ~~OF THE INVENTION~~

[0002] **1. Field** ~~of Invention~~

[0003] The present invention is a wireless ~~biometric~~ broadband interactive gaming system and method. More particularly, the wireless ~~biometric~~ broadband interactive gaming system and method operates in a networked environment that ~~which~~ interfaces with a gaming server and a video server. ~~plurality of network access devices including personal computers, wireless devices, and interactive set top boxes~~.

[0004] **2. Description of Related Art**

[0005] The related art includes gaming devices, on-line gaming, networked interactive gaming, and biometrics.

[0006] **Gaming Devices**

[0007] For purposes of this patent, the term "gaming" shall refer to either gambling and/or gaming applications. Gaming devices include games of skill and games of chance. Games of chance include many casino-type gaming devices in which the outcome of the game depends, at least in part, on a randomly generated event. For example, a game of chance may use a random number generator to generate a random or pseudo-random number. The random number may then be compared to a predefined table to determine the outcome of the event. If the random number falls within a certain range of numbers on the table, the player may win a predefined prize. The table may also contain display information that allows the gaming device to generate a display that corresponds to the outcome of the game. The gaming device may present the outcome of the game on a large variety of display devices, such as mechanical spinning reels or video screens.

[0008] Games of skill comprises a skill component in which a player combines letters or words (word puzzles), answers questions (trivia), overcomes challenges (video games), competes with other players (networked video games), and the like. Generally, a game of skill is a game requiring a level of skill which does not rely solely on chance. Some games of skill require a high degree of expertise and knowledge and other games of skill require very limited expertise or knowledge.

[0009] **On-Line Gaming**

[0010] In June 2001, Nevada signed a bill that could result in Nevada being the first state to offer legalized gambling over the Internet. The new law authorizes state gaming regulators to set up an infrastructure to license and oversee online gaming in Nevada when such gaming becomes legal. Online gaming is a federal issue whose legality is unclear at present.

[0011] A variety of technological limitations have been asserted as preventing Congress's endorsement of on-line gaming. These technological limitations are related to the prevention of underage gambling, the control of gambling addiction, and ensure on-line gaming is secure and reliable.

[0012] To prevent underage gambling prior art systems and methods use passwords, user IDs, credit cards and "click-through" agreements that ask the player to agree to being of legal gambling age by clicking on a button. Presently, there are no systems and methods to control on-line gambling addiction. With respect to ensuring on-line gaming is secure and reliable, prior art system and methods use various cryptographic techniques such as RSA encryption, digital certificates, or other similar well known cryptographic methods. These cryptographic methods are helpful in ensuring secure communications, however these cryptographic method do not ensure that the individual accessing the on-line game is a valid user.

[0013] In view of the prior art systems, a minor or other unauthorized individual may simply needs a user ID and a corresponding password to access a gaming site. The obtaining of a user ID and password is a relatively simple task as this information is generally not modified. Commonly the user ID information is acquired by simply identifying the web site's naming convention for the player. The player password can be easily determined by simply remembering the pattern of keys typed by the player during the log-on procedures or by simply requesting the password from the player as part of a diagnostic procedure. The latter is a trick commonly used by hackers to access a system. The password problem may be overcome by modifying the password on a regular basis, however the player must then remember the modified password and should the player forget the password a new password is mailed. During the mailing process it is common for e-mail to be easily intercepted in cyberspace. Additionally, it is common for unauthorized users to simulate being at a certain location by submitting an IP address that identifies an authorized user.

[0014] Therefore, a better system and method for identifying a valid user is needed. Additionally, it would be beneficial to provide a gaming system and method that would prevent underage gambling, is simple to implement, prevents gambling addiction, and provides a higher degree of security and reliability from unauthorized users.

[0015] **Networked Interactive Gaming**

[0016] Networked interactive gaming III an open networked environment such as the Internet is well-known. However, interactive gaming in an open network such as the Internet is confined to communicating with other devices using the same TCP/IP protocols. Currently networked interactive gaming systems using the TCP/IP protocol are not configured to communicate with interactive set-top boxes using MPEG protocols.

[0017] Networked interactive gaming in an open networked environment using traditional security methods such as secure socket layers and digital certificates are well known. However, networked interactive gaming in an open networked environment using traditional security methods does not prevent gambling from a minor having acquired a parent's user ID and password without the parent's consent.

[0018] Networked interactive gaming using LANs and WANs for progressive slot machines having large jackpots are also well-known. However, networked interactive systems using LANs and WANs for progressive slot machines generally exist in a highly secure proprietary network environment. Thus, the creation of a progressive slot machine with a large jackpot in an open network environment is not well known.

[0019] **Biometrics**

[0020] A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

[0021] Biometric applications for games of skill and games of chance are limited. For example biometric gaming applications are taught in U.S. Pat. 6,010,404 granted to Walker et al. teaches a method and apparatus for using player input codes (e.g., numeric, biometric or physical) to affect the outcomes of electronic gambling devices, such as slot machines. Additionally, U.S. Pat. No. 6,142,876 granted to Cumbers teaches a system and method for passively tracking the play of players playing gaming devices such as slot machines. Players provide identification information and facial recognition data is acquired by a digital or video camera. For each player an account file and a file of the facial image data is stored. When the player plays the slot machine, a camera scans the player and acquires facial image data which is compared to stored data to identify the player. Furthermore, U.S. Patent No.5,902,983 granted to Crevelt et al. teaches a gaming machine configured to perform EFT transactions which are limited to preset amounts. The patent teaches the use of a finger print imaging device, and retinal scans for verifying a player's identity.

[0022] Although biometric applications for gaming applications are known, biometric applications for on-line gaming systems are not known. Furthermore, the managing of biometric information and gaming information in an open network environment are not known. Additionally, the use of biometrics in a gaming system and method to prevent underage gambling and prevent gambling addiction are not known.

SUMMARY ~~OF INVENTION~~

[0023] ~~1. Advantages of the Invention~~ A wireless gaming system comprising a first wireless network access device and a gaming system is described. The first wireless network access device has a plurality of security identification information associated with the first wireless network access device that comprises an Internet Protocol (IP) address. The gaming system is configured to communicate with the first wireless network access device. The gaming system comprises a registration database, a verification system, a video server and a gaming server. The registration database stores registration data associated with each registered user. The verification system is in communication with the wireless network access device and the registration database. The verification system is configured to verify the user is a registered user. The verification system is configured to secure communications with the wireless network access device by verifying the plurality of security information provided by the first wireless network access device including the IP address of the wireless network access device. The video server stores a plurality of images corresponding to a particular game outcome. The gaming server is configured to generate a random game output that associates the random game output with at least one particular game outcome. The gaming server is configured to communicate the images corresponding to the particular game outcome to the first wireless network access device. The gaming server is further configured to be accessible by the wireless network access device after verifying the wireless network device is a secure device, and after verifying the user has registered.

[0024] A wireless gaming system that comprises a plurality of wireless network access devices and a gaming system is also described. The verification system in this embodiment comprises a firewall disposed between a gaming server and each wireless network access device. The video server stores a plurality of different animated images, wherein a group of images corresponds to a particular game outcome. The gaming server is configured to generate a random game output that associates the random game output for one of the wireless network access devices with at least one particular game outcome and the corresponding group of animated images. The gaming server is configured to be accessible by the wireless network access device after verifying each wireless network device is a secure device, and after verifying the user has registered. Additionally, an encoder configures the group of animated images as a video stream that is received by each wireless network device. ~~One of the advantages of the present invention is that it provides a secure and reliable on-line gaming system and method.~~

[0025] A wireless gaming method is also described. The wireless gaming method comprises receiving has a plurality of identification information including an Internet

Protocol (IP) address. The method then proceeds to communicate the plurality of identification information associated with the wireless network access device to a gaming system. The gaming system comprises a registration database that stores registration data associated with each registered user. The method verifies that the user is a registered user. The method also verifies that the wireless network access device is a secure device by verifying the plurality of identification information associated with the wireless network access device that comprises verifying the IP address. Access to the gaming server is permitted after determining the wireless network device is secure and after determining the user has registered. A random game output is generated at the gaming server. The random game output is associated with a particular game outcome. Images corresponding to a plurality of game outcomes are stored on a video server. The particular game outcome is associated with a plurality of corresponding images and the corresponding images are communicated to the wireless network access device. ~~A further advantage of the present invention is that it provides a secure system and method for identifying a user in an open network environment.~~

[0026] A further advantage of the present invention is that it provides a system and method to prevent underage gambling.

[0027] A further advantage of the present invention is that it provides a more secure and reliable and secure gaming system and method.

[0028] Another advantage of the present invention is that it provides a system and method for managing biometric information and gaming information in an open network environment.

[0029] Another advantage of the present invention is that it permits a plurality of users in a geographically broad area to play the same game.

[0030] A further advantage of the present invention is that it provides a pseudo-real time gaming system and method.

[0031] Another advantage of the present invention is that it simulates a game of chance such as a slot machine in an on-line environment.

[0032] An additional advantage of the present invention is that it provides a networked jackpot.

~~2. Brief Description of the Invention~~

[0033] ~~The present invention is a~~ A networked gaming system that comprises a verification system, a broadband gaming system and a transactional system is described. The verification system operations include ensuring that a user is a registered player by using a biometric input. The broadband gaming system operations include managing and performing at least one game. The transactional system operations include providing oversight for each transaction conducted by the verification system and the broadband gaming system.

[0034] ~~The present invention comprises a~~ A verification system for playing the networked gaming system is described. The networked games include games of chance and games of skill. The verification system communicates with a biometric input module and a network access device to generate a user identification information. The user identification information is compared to information in a registration database. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to both the broadband gaming system and the transactional system.

[0035] ~~Additionally, the present invention includes a~~ A broadband gaming system which is in communication with the verification system is described. The broadband gaming system includes a buffer which stores information about players who desire to play a game. The buffer is operatively coupled to a random number generator that generates a random number for each player in the buffer. A paytable module in communication with the random number generator determines the outcome associated with the random number generator. The paytable also determines which images associated with the outcome for each player. Preferably, the images are stored on a mini video server and then cached in a memory module. The images are intelligently buffered for downstream communications. In its preferred embodiment, a plurality of encoders are operatively coupled to the memory module caching the broadcast video streams. The plurality of encoders encode the broadcast downstream images according the requirements for each network access device. Each encoder ~~encoders~~ is operatively coupled to an encryption module that encrypts the broadcast. A modulation module is operatively coupled to the encryption module and modulates encrypted images for downstream transmission. Each network access device includes a tuner, a demodulation module, and a decryption module permits an image to be viewed by the network access device.

[0036] ~~Further still the present invention provides a~~ A transactional system and method that ensures secure communications occur in the verification system and the broadband gaming system is described. The transactional system also performs accounting, bonusing, tracking and other such functions. Preferably, the transactional system is capable of receiving a plurality of funds from a financial account and converting them to credits that are used in the broadband gaming system.

[0037] The above description sets forth, rather broadly, the more important features of the present invention so that the detailed description of the preferred embodiment that follows may be better understood and contributions of the present invention to the art may be better appreciated. There are, of course, additional features of the invention that will be described below and will form the subject matter of claims. In this respect, before explaining at least one preferred embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of the construction and to the arrangement of the components set forth in the following description or as illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

BRIEF DESCRIPTION OF THE DRAWINGS

[0038] Preferred embodiments of the present invention are shown in the accompanying drawings wherein:

[0039] FIG. 1*a* through FIG. 1*d* provide diagrams of a plurality of network access devices.

[0040] FIG. 2 is a high level diagram of a gaming system networked to a plurality of network access devices.

[0041] FIG. 3 is a block diagram of an illustrative biometric input module.

[0042] FIG. 4 is a block diagram of a gaming system configured to receive a biometric input from a network access device.

[0043] FIG. 5 is a table of the data fields in a verification system.

[0044] FIG. 6 is a table of the data fields in a broadband gaming system and in a transactional system.

[0045] FIG. 7 is a block diagram of a broadband gaming system.

[0046] FIG. 8 is a flowchart of the registration method for the gaming system.

[0047] FIG. 9 is a flowchart of the verification method for the gaming system.

[0048] FIG. 10 is a flowchart of the information processed by the gaming system. ~~gaming method for the gaming system.~~

[0049] FIG. 11 is a continuation of the flowchart of the information processed by the gaming system in FIG. 10. ~~is a flowchart of the method for purchasing credits for the gaming system.~~

~~FIG. 12 is a flowchart of the method for storing credits on the gaming system.~~

~~FIG. 13 is a flowchart of the information processed by the broadband gaming system.~~

~~FIG. 14 is a continuation of the FIG. 13 flowchart.~~

~~FIG. 15 is a flowchart of the information processed by the transactional system in communication with the broadband gaming system.~~

DESCRIPTION ~~OF THE PREFERRED EMBODIMENT~~

[0050] In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings, which form a part of this application. The drawings show, by way of illustration, specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

[0051] NETWORK ACCESS DEVICES

[0052] Referring to FIG. 1*a* through FIG. 1*d* there is shown a plurality of illustrative network access devices. Each of the network access devices is configured to be capable of running a gaming application. For illustrative purposes the gaming application shown simulates the spinning reels of a slot machine.

[0053] The network access device in FIG. 1*a* is a personal computer 10 having a network interface card (not shown) that may be operatively coupled to a modem (not shown). Another network access device shown in FIG. 1*b* includes a television 12 operatively coupled to an interactive set-top box 14 that is operatively coupled to a cable network (not shown). The other network access device shown in FIG. 1*c* is a wireless device 16 such as a digital phone or personal digital system (PDA) or other such wireless device which is configured to communicate with a network using wireless networking protocols. Yet another network access device is shown in FIG. 1*d* and includes a gaming terminal 18 such as a slot machine on a casino floor that is operatively coupled to a plurality of other gaming terminals. It shall be appreciated by those skilled in the art of networking that the distinguishing feature between each of these network access devices is the type of communications protocols used by each device to enable communications between similar network access devices.

[0054] Each of the network access devices either includes a biometric input module operatively coupled to the network access device or includes a biometric input module communicatively coupled to the network access device. A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

[0055] In one illustrative embodiment, the biometric input module is a fingerprint scanner 20 resident on the gaming terminal 18 wherein the biometric input is a fingerprint. In another illustrative embodiment, the biometric input module is the screen 22 of wireless device 16 wherein the screen is configured to receive a biometric input such as a user signature. In yet another illustrative embodiment, the biometric input module is a telephone 24 that is configured to receive a voice pattern from a user prior to engaging communications with the interactive set-top box 14. In yet another illustrative embodiment the biometric input module is a keyboard 26 operatively coupled to computer 10 wherein the user is requested to input a keystroke pattern. An illustrative example of a biometric input module operatively coupled to the network access device is shown in FIG. 1*d* having the fingerprint scanner 20 on the gaming terminal 18. An illustrative example of a biometric input module, e.g. the telephone 24, communicatively coupled to the network access device, e.g. the interactive set-top box 14, is shown in FIG. 1*b*.

[0056] The biometric input is used to prevent unauthorized gaming activity and efficiently store credits on the user's behalf. By way of example and not of limitation, unauthorized gaming activity includes preventing underage gaming and prohibiting a player with a history of gambling addiction from playing games of chance. Additionally, player credits may be stored on a network so that the player does not need to carry coins, paper currency, coupons, credit cards or debits cards to play a game. It shall be appreciated by those skilled in the art having the benefit of this disclosure that different biometric input modules may be used in conjunction with different network access devices.

[0057] **GAMING SYSTEM**

[0058] Referring to FIG. 2 there is shown a high level block diagram of a gaming system 30 in communication with a plurality of network access devices coupled to a network 32. The gaming system includes a verification system 34, a broadband gaming system 36 and a transactional system 38. The verification system 34 verifies that a user operating a network access device is a registered player. The broadband gaming system 36 performs the function of generating a game and broadcasting the game results to each of the network access devices. The transactional system 38 performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system and conducting electronic fund transfers.

[0059] **Verification System**

[0060] The verification system 34 verifies that a user desiring to play the game is a registered player. The verification system 34 communicates with the biometric input module and a network access device to generate [[a]] user identification information. The user identification information includes information such as cryptographic keys that are necessary to securely identify the network access device. The user identification information also includes media access control (MAC) identification and confirmation of the user Internet Protocol (IP) address. The user identification information is compared to information in a registration database 40 by a verification server 42. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to either the broadband gaming system 36 or the transactional system 38.

[0061] In an alternative embodiment the user identification information is housed in a smart card (not shown) that is communication with the verification system 34. The smart card includes a stored biometric which is used to identify the user as a player. Cryptographic keys are then exchanged between the verification system 34 and the smart card to provide the player access to either the broadband gaming system or the transactional system 38.

[0062] Referring to FIG. 3 there is shown an illustrative biometric input module 50. By way of example, the illustrative biometric input module 50 is a fingerprint scanner. It shall be appreciated by those skilled in the art having the benefit of this disclosure that the use of the fingerprint scanner as the illustrative biometric input module is not restrictive. A scanned fingerprint image is collected by the biometric input 52. After the scanned fingerprint image is collected, the fingerprint image is compressed by the compression module 54. A memory module 56 provides fast memory resources for the compression of the fingerprint image. After compression, the fingerprint image is encrypted by the encryption module 58 for downstream transmission. The encryption module 58 also includes a memory module 60 that provides fast memory resources for the encryption of the compressed fingerprint image. An encrypted compressed fingerprint image is then communicated to network 32 (see FIG. 2) using the network interface module 62.

[0063] Referring to FIG. 4 there is shown a block diagram of the verification system 34. The verification system is operatively coupled to network 32 with network interface module 64. The network interface module 64 is configured to receive user identification information generated by the network access devices and from the biometric input module. Preferably, the biometric and other user identification information received by the verification system is an encrypted biometric that is decrypted by decryption module 66. A memory module 68 is preferably a fast memory that expedites the decryption process. After decryption the biometric and remaining user identification information is processed by the verification server. It shall be appreciated by those skilled in the art that the verification server 42 may house the network interface module 64, decryption module 66 and the memory module 68. The verification server 42 is also in operative communication with a registration database 40. The verification server 42 performs the function of matching the user identification information collected from the network access device with the player information in the registration database 40. Additionally, the verification server 42 performs the caching functions needed to ensure that once a player has been identified during an initial game, subsequent usage by the same player proceeds quickly.

[0064] Preferably, the verification server 42 identifies registered players using a biometric template of the registered player residing on the registration database 40. The registered players are referenced with Personal ID number. When a transaction is undertaken the user firstly calls up the particular template from the registration database 40 by inputting a Personal ID. The Personal ID includes a particular number, user ID, password or other such identification techniques. The inputting of the Personal ID is accomplished with a familiar numeric keypad, keyboard, magstripe card or smart card. The correct template is called and held in memory ready for comparison with the biometric sample provided by the user. A comparison takes place that results in a binary true or false condition as to the identity of the user. The user is in effect claiming an identity by inputting the Personal ID and the system is subsequently verifying that the claim is genuine according to the matching criteria setup within the system.

[0065] Referring to FIG. 5 there is shown the registration data fields 70 and user submitted data fields 72. The registration data fields 70 include data fields that comprise the user identification information. The registration data fields include user identification information such as player name, address, user name, password, credit card information, and the date and time of the registration. The player biometric and Personal ID also comprises the user identification information and provides unique information about the player. The Personal ID may be the same as the user name or password. It shall be appreciated by those skilled in the art that some biometric information may be compressed. Furthermore, the user identification information includes data about the network access device and the network connection such as MAC ID, IP addresses, browser type, any cookies resident on the network access device, etc. Finally, the user identification system includes cryptographic keys which are used to encrypt and decrypt the communications between the verification system and each of the network access devices.

[0066] The user submitted data fields 72 mirror the registration data fields 70. The user submitted data fields receive data generated by a user that is attempting to access the broadband gaming system 36. The user submitted information is carefully analyzed to ensure that a valid user is being identified. It is well known that the connection of one network access device to another network access device generates security concerns. Preferably, the present verification system operates using a fast hardware-type firewall that performs a stateful multilayer inspection. In its preferred embodiment the firewall provides packet filtering using a secure protocol such as IPSec. This protocol provides encryption of the data at the packet level as well as at the source address level. Without access to the encryption keys, a potential intruder would have difficulty penetrating the firewall. Additionally, it would be preferable to provide a circuit level gateway and an application level gateway. The circuit level gateway works on the session layer of the OSI model or the TCP layer of the TCP/IP model and monitors TCP handshaking between packets to determine whether a requested session is legitimate. The application level gateway filters data packets at the application layer of the OSI model. A stateful multilayer inspection firewall offers a high level of security, good performance and transparency to end users.

[0067] Referring to FIG. 6 there is shown the player data fields 74 that are generated by the broadband gaming system and the transactional system after the user has been verified to be a registered player. The player data fields 74 are used to generate a player matrix which is used as an additional internal security measure. The player data fields 74 include a Player ID that identifies the player, a timestamp that provides the date, time in and time out by the player during the game. Additionally, the type of game, credits played, and credits remaining are monitored. Based on the level of player activity a bonus is provided to the player. Further still the session time for each type of game and the amount played during the session is monitored to better define the type of games the players' like. Transactional information is also monitored and updated, preferably, by the transactional system 38. The transactional information includes credit card information, transaction requests, transaction approval, conversion of monetary funds to credits for playing the game, any transfers of credits for playing the game, and conversions from credits to monetary funds that are credited to the player's financial account. Preferably, communications between the transactional system and the broadband gaming system are conducted in a secure environment using cryptographic keys. Although the use of cryptography within the private network may appear excessive one of the greatest security threats within a private network comes from its own employees. Therefore, it is preferable to use internal firewalls for communications between the broadband gaming system, the transactional system and the verification system.

[0068] **Broadband Gaming System**

[0069] A more detailed drawing of the broadband gaming system is provided in FIG. 7. The dashed boundary in FIG. 7 defines the broadband gaming system 36. After player verification is completed at the verification system 34, the broadband gaming system 34 is engaged. The broadband gaming system 34 includes a player buffer 84 configured to receive the players who will be playing the game. The player buffer 84 generates an initial player matrix with player data
fields 74.

[0070] A countdown timer 82 is coupled to the player buffer 80. Preferably, the countdown timer 82 is also displayed to the player. The countdown timer 82 provides a window of time within which players may join the game. The players that have joined the game before the end of the timing period are stored in the buffer. When the timing period reaches zero the initial player matrix is communicated to the transactional system 38 and to the gaming module 84.

[0071] The gaming module 84 provides a game that is played by the plurality of players. The game may include a plurality of different games and the type of game is not restrictive to this invention. Preferably, the gaming module 84 includes at least one random number generator 86 and a paytable module 88.

[0072] The random number generator 86 is operatively coupled to the player buffer. The random number generator 86 generates at least one random number that is stored in the player matrix. In one embodiment, at least one random number is generated for the plurality of players playing the game. In an alternative embodiment, at least one random number is generated for each player. In yet another embodiment, a plurality of random numbers are generated that are applied to the plurality of players playing the game. Preferably, the random number generator 86 is a fast hardware module.

[0073] A paytable module 88 is operatively coupled to the random number generator 86. The paytable module 88 is a programmable module that determines the type of prize awarded to the player based on the random number generated by the random number generator 86. In one embodiment, the paytable module 88 is a field programmable gate array. Preferably, the paytable module 88 also includes an image ID that is associated with the outcome determined by the paytable module 88.

[0074] A gaming output module 90 revises the player matrix to include the outcome for each player. Additionally, the gaming output module 90 groups the players according to the image ID. Based on the results generated by the gaming module 84, the gaming output module 84 generates a final player matrix that is communicated to the transactional server 38 and to a memory module 92.

[0075] Preferably, the memory module 92 has stored a plurality of images in a fast memory by the time the final player matrix is communicated to the memory module 92. In operation, the memory module 92 is enabled before the final matrix is communicated to the memory module 92. By way of example, when the game is engaged the memory module 92 begins the process of finding the applicable images associated with the image IDs in the mini-video server 94 and transferring the images to the fast memory module 92. Thus, when the gaming output is received by the memory, the images are stored in the fast memory module 92. In one embodiment, the memory module 92 then broadcasts the images to encoders 96 and 98. In an alternative embodiment, the memory module 92 is operatively coupled to an intelligent router (not shown) that routes the images to the appropriate encoders 96 and 98.

[0076] The appropriate encoder then receives the images and converts them to a format which meets the requirements for the appropriate network access device. By way of example, an IP encoder 96 encodes a plurality of JPEG images for viewing on a conventional web browser, and an MPEG encoder 98 encodes the plurality of JPEG images into an MPEG stream that is viewed on a television via an interactive set-top box.

[0077] An encryption module 100a and 100b operatively coupled to encoder 96 and 98, respectively, then receives the encoded images and encrypts the encoded images in manner well known to those skilled in the art. A modulation module 102a and 102b is operatively coupled to encryption modules 100a and 100b, respectively, then modulates encrypted encoded images for downstream transmission in a manner well known to those skilled in the art.

[0078] Preferably, the broadband gaming system occupies one downstream band, i.e. one 6 or 8 MHz band, in the interactive set-top-box environment. In the web based broadcast environment, the broadband gaming system occupies a downstream channel much like a standard streaming media website.

[0079] It shall be appreciated by those skilled in the art having the benefit of this disclosure that the broadband gaming system can play more than one game at a time. The system may be designed to operate in a multi-tasking mode where more than one game is played at a time. Additionally, the system may be designed to operate in a fast serial mode in which a game is played while the countdown timer is waiting for the next queue to be filled.

[0080] **Transactional System**

[0081] Referring back to FIG. 2, there is shown the transactional system 38 which comprises a transactional server 110 and a transactional database 112. The transactional system 38 performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system. Additionally, the transactional system 38 is configured to authorize and conduct electronic fund transfers. Furthermore, the transactional system 38 performs such operations as player tracking, managing loyalty programs, engaging bonus games, determining bonus prizes and interfacing with accounting programs.

[0082] **METHOD FOR REGISTERING A PLAYER**

[0083] Referring to FIG. 8 there is shown a flowchart of the registration method for the gaming system 30. The registration method 150 begins when a prospective player first accesses a website, channel, kiosk or other such registration terminals as described in block 152. The method then proceeds to block 153.

[0084] At block 153, the registration process is initiated. By way of example and not of limitation, a registration terminal may provide a hyperlink to a registration window that prompts the prospective player for information. The method then proceeds to block 154.

[0085] At block 154, the prospective player provides registration identification information such as name, address, credit card number and other information necessary to create a registration file for the prospective player. The method then [[the]] proceeds to block 156.

[0086] At block 156, the prospective player is prompted for a personal ID. The personal ID may be a user ID, a password, a numeric combination, or any other such identification information. The personal ID is used during the verification process to identify a biometric template for the prospective player. The method then proceeds to block 158.

[0087] At block 158, the prospective player submits a biometric to the registration terminal. By way of example and not of limitation the biometric is a fingerprint. Any other biometric may also be used. The method then proceeds to block 160 or 162.

[0088] At block 160, the biometric input is compressed and encrypted. It is preferable for certain biometric inputs to compressed such as fingerprint scans, retinal scans and other such scanning techniques. Other biometric inputs such as voice patterns, signatures do not have to be compressed. The process of encrypting biometric inputs is necessary in an open network environment. The process of encrypting may not be necessary on a private proprietary network. Therefore, it shall be appreciated by those skilled in the art having the benefit of this disclosure that the compression and encryption processes in block 160 may not be necessary for every biometric input.

[0089] At block 162, the prospective player information is stored in the verification system and a player profile is updated accordingly. Alternatively, the prospective player information is stored on a smart card. The method then proceeds to block 164.

[0090] At block 164, security information about the registration terminal is collected. The registration information identifies the registration terminal as being a secure terminal. The registration terminal provides information such as the MAC ID for the biometric input module, the IP address for the server communicating with the registration terminal, and the cryptographic keys associated with the registration terminal. The registration terminal includes the network access devices described in FIG. 1*a* through FIG.1*d* as well as kiosks and other such registration terminals.

[0091] At block 166, the prospective player is identified as a registered player and the registration database 40 is updated accordingly. The registration process is broken out into separate components for security purposes. Once a validly registered player is identified by the verification system, the registration process is completed.

[0092] METHOD FOR PLAYER VERIFICATION

[0093] Referring to FIG. 9 there is shown a method 170 for player verification used by the verification system 34. The player verification process includes receiving user identification information from a network access device. The method is initiated at block 174 when a user accesses a website or channel displaying the game. The method then proceeds to block 176.

[0094] At block 176, the personal ID is provided by the user. The personal ID is used by the verification system to find a biometric template for determining whether the user is a registered player. The method then proceeds to block 178.

[0095] At block 178, the biometric input module of the network access device receives a biometric from the user. As previously described the biometric input module can be one of plurality of biometric inputs. Depending on the type of biometric, the biometric may be compressed as described by block 180 and encrypted as described by block 182. At block 184, the biometric and the personal ID is then communicated through a network 32 to the verification system 34. Alternatively, the biometric and Personal ID is communicated to a smart card for verification.

[0096] At block 186, the verification system 34 requests security information from the network access devices. The security information identifies the network access devices as being a valid network access device. The method then proceeds to block 188.

[0097] At block 188, the verification system 34 processes the security information to ensure that the security information is generated by the appropriate network access device, and to ensure that the security information has not been compromised. Preferably, the verification system 34 performs a stateful multilayer inspection as described above. The method then proceeds to block 190.

[0098] At block 190, the user submitted player information is compared to the registered player information. If a determination is made at decision diamond 192 that the submitted player information is not a valid registered player the method proceeds to block 194. At block 194, the user is requested to re-input the biometric. If the biometric is input more than three times, as provided by decision diamond 196, the user is requested to contact customer service.

[0099] If a match is found at decision diamond 192 between the user submitted information and the registered player information, the user is identified as a valid player then the player proceeds to the broadband gaming system 36.

[0100] METHOD FOR OPERATION OF BROADBAND GAMING SYSTEM

[0101] Referring to FIG. 10 and FIG. 11 there is shown a flowchart 200 of the information processed by the broadband gaming system 34. The process is engaged by performing the verification process in which the verification system identifies a player as in block 201. After the verification process has been completed the method proceeds to block 202.

[0102] At block 202, the players who desire to play a particular game are stored in a buffer until the particular game is engaged. The method then proceeds to decision diamond 204.

[0103] At decision diamond 204, the countdown timer 82 determines if the period during which the game is open has been closed. If the game remains open, additional players may be received by the broadband gaming system. If the game ~~games~~ is closed because the period during which the game is open has expired, then the method proceeds to block 206.

[0104] At block 206, the initial player matrix described above is generated. The initial player matrix includes information about the player, the type of game, and other such information about the game as described by the player data fields 74 shown in FIG. 6. The initial player matrix is then communicated to block 208 which transmits initial player matrix to the transactional system for validation. Additionally, the initial player matrix is communicated to the next block 210 in the broadband gaming system which starts the gaming module.

[0105] At block 210, the initial player matrix is received by the gaming module 84 and the gaming module 84 is engaged. At a minimum the gaming module 84 comprises a random number generator 86 and a paytable module 88. The random number generator generates at least one random number that is used during the game. The paytable module 88 is used to determine the prize associated with the at least one random number.

[0106] Referring to FIG. 11, a continuation of the broadband gaming system method is shown. By way of example, the gaming module may comprise a plurality of different random number generators. The blocks 214 and 216 describe the processes performed by a random number generator and a paytable module, respectively. The random number generator 86 of block 214 determines the winning combination of numbers for the game. At block 216, the paytable module 88 is used to determine the prize awarded to the player. Preferably, the paytable module 88 is also configured to prov[[e]]ide image IDs that identify the images associated with the prize. Preferably, the paytable module 88 is resident in both the broadband gaming system and the transactional system. The purpose for this redundancy is as a security check for output generated by the gaming module. The method then proceeds to block 218.

[0107] At block 218 the player outputs with the same image IDs are grouped together. The grouping process is performed to simplify the broadcasting of the images to the plurality of players. By grouping the players according to the same image ID and having identified the network access device used by the player, a dynamic broadcasting method is created which occupies minimal downstream bandwidth. The method then proceeds to block 220.

[0108] At block 220 a final player matrix is completed. The final player matrix includes the same data fields as the initial player matrix. Additionally, the final player matrix includes the random number output and the paytable output. The final player matrix is then communicated to the transactional system as described in block 222. The method then proceeds to decision diamond 224.

[0109] At decision diamond 224, a validation procedure is conducted. The validation procedure essentially compares the transactional system's reverse calculation of the random numbers with the random numbers generated by the gaming module. If the random numbers in the transactional system are not the same or similar to the random numbers generated by the random number generator, a system failure or security breach is detected. If a security breach or system failure is detected, the method then proceeds ~~proceed~~ to process block 226, which initiates diagnostic procedures. If the random numbers match, then the method proceeds to block 228.

[0110] At block 228, the plurality of images are broadcast. The images are preferably broadcast along one downstream channel for each network access device. However, traffic considerations may require the use of a plurality of downstream channels. By way of example, for DOCSIS and DSL type downstream transmissions, the streaming video preferably occupies a portion of the bandwidth available for a cable modem or DSL modem, respectively. In an alternative example, for an interactive set-top box environment, the downstream channel preferably occupies one 6 MHz or 8 MHz band or a portion of the 6 MHz or 8 MHz band. The method then proceeds to the next block 230.

[0111] At block 230, the broadcast images are encoded for downstream transmission. It shall be appreciated by those skilled in the art having the benefit of this disclosure that downstream transmission systems are well known and can be easily integrated into the systems and method described in this patent. The method then proceeds to block 232.

[0112] At block 232, the broadcast images are encrypted for downstream transmission. The purpose for downstream encryption is to prevent unauthorized access to the downstream signal. It shall be appreciated by those skilled in the art that various secure systems and methods for downstream transmission of images are well known.

[0113] It shall be appreciated by those skilled in the art having the benefit of this disclosure that a plurality of games may be played simultaneously. The games may be played in a distributed/parallel manner or in serial manner.

[0114] **AN ILLUSTRATIVE GAME**

[0115] An illustrative game is described to show how the system and method described above operates. The illustrative game described herein is a progressive slot machine. It is well-known that in the United States many states have legalized lottery games even though other games of chance such as progressive slot machines have not been legalized. It is also well-known that in casino gaming floors the most popular games are progressive slot machines. The present illustrative game operates on the system and method described above and provides an output similar to a progressive slot machine with a lottery type input.

[0116] The illustrative game includes first having a player provide a plurality of letters or numbers that are either generated by the player or are selected in a random manner. The random number generator of the gaming module is then engaged and a gaming module random number is generated. Preferably, the order that the random numbers were generated is used to determine the prize awarded to the player. A programmed paytable is then used to compare the player selected numbers to the gaming module random numbers according to the rules programmed into the paytable module. Based on the results of this comparison a prize is awarded to the player. An image ID is associated with the prize awarded. The plurality of players are then grouped according to their respective image IDs. A broadcast stream for the plurality of images associated with each image ID is broadcast to each player.

[0117] A more concrete example includes having a player select a plurality of numbers, such as the numbers below:

25 35 8 15 42

[0118] The random number generator of the gaming module is then engaged. By way of example the random number results are:

56 2 3 8 42

[0119] The paytable module is then programmed to interpret the random numbers generating by the gaming module according to the following illustrative rules:

[0120] 1. If a match between one number is achieved, then a prize of Ix the initial bet credit is awarded and an image ID XQ23-1396 is used. Image ID XQ231396 is an animated plurality of images representing three cherries.

[0121] 2. If a match between one number at the same location is achieved, then a prize of 2x the initial bet credit is awarded and an image ID XQ23-1397 is used. Image ID XQ23-1397 is an animated plurality of images representing four cherries.

[0122] 3. If a match between a first number is achieved and a match between a second number is achieved, then a prize of 5x the initial credit is awarded and an image ID XQ23-1998 is used. Image ID XQ23-1998 is an animated plurality of images representing 3 oranges.

[0123] 4. If a match between a first number at the same location is achieved and a match between a second number is achieved, than a prize of 7x the initial credit is awarded and an image ID XQ23-1999 is used. Image ID XQ23-1999 is an animated plurality of images representing 4 oranges.

[0124] Thus, for the illustrative example provided above, the player having selected the numbers: 23, 35, 8, 15 and 42 is entitled to a prize of 7x the initial credit for a random number: 56,2,3,8, and 42. The associated images displayed on the network access device is an animated plurality of images representing 4 oranges.

~~CONCLUSION~~

~~It can now be seen that the present invention solves many of the problems associated with the prior art. The present invention provides a verification system that uses biometrics to identify the player. The present invention provides a broadband gaming system that communicates with a plurality of different network access devices. Furthermore, the present invention provides a system and method~~

~~for generating a combined jackpot in an open network environment across a broad geographical area.~~

~~Although the description above contains many specifications, these should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention. The specification, for instance, makes reference to bonus prizes. However, the present invention is not intended to be limited to bonus prizes. Rather it is intended that the present invention can be used independently as a stand-alone game. Thus, the~~ The scope of the invention should be determined by the appended claims and their legal equivalents rather than by the examples given.

ABSTRACT

~~The present invention is a biometric broadband gaming system and method that comprises a verification system, a broadband gaming system and a transactional system. The verification system operations include receiving a biometric input to ensure that a user is a registered player. The broadband gaming system operations include providing a game of skill or game of chance to a plurality of players communicating via different network access devices. The transactional system operations include managing transactions conducted by the verification system and the broadband gaming system.~~

A wireless broadband gaming system and method is described. The wireless broadband gaming system includes a wireless network access device and a gaming system. The gaming system includes a registration database, a verification system, a video server and a gaming server. The video server stores images corresponding to at least one particular game outcome. The gaming server generates a random game output that associates the random game output with at least one particular game outcome. The gaming server communicates the images corresponding to the particular game outcome to the wireless network access device after verifying the wireless network device is a secure device and after verifying the user has registered.